Carmen's Core Concepts (Math 135)

Carmen Bruni

University of Waterloo

Week 7 Part 2

Definition of a Commutative Ring and Field

Definition: A commutative ring is a set R along with two closed operations $+$ and $\cdot$ such that for $a, b, c \in R$ and

1. Associative $(a+b)+c = a+(b+c)$ and $(ab)c = a(bc)$.
2. Commutative $a+b = b+a$ and $ab = ba$.
3. Identities: there are [distinct] elements $0, 1 \in R$ such that $a+0 = a$ and $a \cdot 1 = a$.
4. Additive inverses: There exists an element $-a$ such that $a+(-a) = 0$.
5. Distributive Property $a(b+c) = ab+ac$.

Example: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$. Not $\mathbb{N}$

Definition of a Commutative Ring and Field

Definition: A commutative ring is a set R along with two closed operations $+$ and $\cdot$ such that for $a, b, c \in R$ and

1. Associative $(a+b)+c = a+(b+c)$ and $(ab)c = a(bc)$.
2. Commutative $a+b = b+a$ and $ab = ba$.
3. Identities: there are [distinct] elements $0, 1 \in R$ such that $a+0 = a$ and $a \cdot 1 = a$.
4. Additive inverses: There exists an element $-a$ such that $a+(-a) = 0$.
5. Distributive Property $a(b+c) = ab+ac$.

Example: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$. Not $\mathbb{N}$

Definition: If in addition, every nonzero element has a multiplicative inverse, that is an element a^{-1} such that $a \cdot a^{-1} = 1$, we say that R is a field.

Example: $\mathbb{Q}$, $\mathbb{R}$. Not $\mathbb{N}$ or $\mathbb{Z}$.

Congruence Classes

Definition: The congruence or equivalence class modulo m of an integer a is the set of integers

$$[a] := \{x \in \mathbb{Z} : x \equiv a \pmod{m}\}$$

$:=$ means "defined as".

Further, define

$$\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z} := \{[0], [1], ..., [m-1]\}$$

The Ring $\mathbb{Z}_m$

We turn

$$\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z} := \{[0], [1], ..., [m-1]\}$$

into a ring by defining addition and subtraction and multiplication by $[a] \pm [b] := [a \pm b]$ and $[a] \cdot [b] := [ab]$. This makes $[0]$ the additive identity and $[1]$ the multiplicative identity. Note that the $[a+b]$ means add then reduce modulo m.

Definition: The members $[0], [1], ..., [m-1]$ are sometimes called representative members.

Definition: When $m = p$ is prime, the ring $\mathbb{Z}_p$ is also a field as nonzero elements are invertible (we will see this later).

Well-Defined

Abstractly: Suppose that over $\mathbb{Z}_m$, we have that $[a] = [c]$ and $[b] = [d]$ for some $a, b, c, d \in \mathbb{Z}$. Is it true that $[a + b] = [c + d]$ and $[ab] = [cd]$?

Well-Defined

Abstractly: Suppose that over $\mathbb{Z}_m$, we have that $[a] = [c]$ and $[b] = [d]$ for some $a, b, c, d \in \mathbb{Z}$. Is it true that $[a + b] = [c + d]$ and $[ab] = [cd]$?

Concretely: As an example, in $\mathbb{Z}_6$, is it true that $[2][5] = [14][-13]$?

Well-Defined

Abstractly: Suppose that over $\mathbb{Z}_m$, we have that $[a] = [c]$ and $[b] = [d]$ for some $a, b, c, d \in \mathbb{Z}$. Is it true that $[a+b] = [c+d]$ and $[ab] = [cd]$?

Concretely: As an example, in $\mathbb{Z}_6$, is it true that $[2][5] = [14][-13]$?

Proof: Note that in $\mathbb{Z}_6$, we have

$$\text{LHS} = [2][5] = [2 \cdot 5] = [10] = [4]$$

and also

$$\text{RHS} = [14][-13] = [14(-13)] = [-182] = [-2] = [4]$$

completing the proof. ■

Addition Table

Addition table for $\mathbb{Z}_4$

$+$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$
$[1]$	$[1]$	$[2]$	$[3]$	$[0]$
$[2]$	$[2]$	$[3]$	$[0]$	$[1]$
$[3]$	$[3]$	$[0]$	$[1]$	$[2]$

Multiplication Table

Multiplication table for $\mathbb{Z}_4$

$\cdot$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[3]$
$[2]$	$[0]$	$[2]$	$[0]$	$[2]$
$[3]$	$[0]$	$[3]$	$[2]$	$[1]$